Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview

Zhang, J., Duong, T. Q., Woods, R., & Marshall, A. (2017). Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy*, *19*(8), [420]. https://doi.org/10.3390/e19080420

Published in:
Entropy

Document Version:
Publisher's PDF, also known as Version of record

entropy

MDPI

Review

Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview

Junqing Zhang [1,*], Trung Q. Duong [1], Roger Woods [1] and Alan Marshall [2]

[1] School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT9 5AH, UK; trung.q.duong@qub.ac.uk (T.Q.D.); r.woods@qub.ac.uk (R.W.)

[2] Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, UK; Alan.Marshall@liverpool.ac.uk

* Correspondence: jzhang20@qub.ac.uk; Tel.: +44-28-9097-6597

Received: 3 July 2017; Accepted: 16 August 2017; Published: 18 August 2017

Abstract: The security of the Internet of Things (IoT) is receiving considerable interest as the low power constraints and complexity features of many IoT devices are limiting the use of conventional cryptographic techniques. This article provides an overview of recent research efforts on alternative approaches for securing IoT wireless communications at the physical layer, specifically the key topics of key generation and physical layer encryption. These schemes can be implemented and are lightweight, and thus offer practical solutions for providing effective IoT wireless security. Future research to make IoT-based physical layer security more robust and pervasive is also covered.

Keywords: Internet of Things; physical layer security; key generation; physical layer encryption

1. Introduction

The Internet of Things (IoT) aims to allow ubiquitous connections between things with computing, communication, and sensing ability. IoT applications include smart cities, smart traffic, healthcare, smart home, industrial monitoring, and environment monitoring, etc., [1,2], which have revolutionized every aspect of our life. On the other hand, many open research problems still remain to allow this technology to become widely available, as proposed in [3]. For example, IoT security and privacy remain a major concern as indicated by the UK IoT government report [4] and agreed by many experts [5]. To this end, research into effective IoT security remains a key objective as indicated by major sponsors such as the US National Science Foundation [6], the European Horizon 2020 research programs [7], and the UK's Engineering and Physical Sciences Research Council [8].

The number of connected devices has already exceeded the world's population and is increasing exponentially. It is predicted by numerous sources that IoT devices will number 10 billion by 2020 [9]. For example, Cisco estimated that there would be 6.58 connected devices per person by 2020, i.e., about 50 billion devices in total [10]. With the huge amount of IoT devices, wireless communication is preferred as it allows easy installation and provides ubiquitous connection. Wireless air interfaces involved in the IoT include IEEE 802.15.4 (Zigbee), Bluetooth Low Energy (BLE), IEEE 802.11 Wi-Fi, LoRaWAN, cellular connections, ultrawide band, near field communication (NFC), radio-frequency identification (RFID), to name but a few.

While we are enjoying the benefits that wireless connection has brought, its broadcast nature makes the transmission vulnerable to passive eavesdropping and active jamming. Thus, there is a clear need to protect the data on-the-fly in the IoT as it will generally contain sensitive, private or confidential information. For example, in healthcare applications, the sensor nodes collect patients' health information such as heart rate and blood pressure. This information is private and highly confidential, and hence a secure transmission channel is required. However, IoT systems are far from

safe and many vulnerabilities exist [11]. For example, HP reported that 70% of devices did not encrypt their communications [12].

The security countermeasures are mainly categorized into computational security and information-theoretic security [13]. The former has been the main approach in protecting the communication systems where cryptographic algorithms and protocols are deployed at the upper layers of the protocol stack [14]. For example, the transport layer security (TLS) is a well-known protocol to protect the transport link [15] while Wi-Fi protected access (WPA) is designed to secure the media access control (MAC) layer in the IEEE 802.11 systems [16]. In IEEE 802 the open systems interconnection (OSI) data link layer is splitted into MAC sublayer and logical link control (LLC) sublayer. A classical cryptosystem comprises public key cryptography (PKC) for key distribution and symmetric encryption for data protection, as shown in Figure 1, where Alice and Bob are the legitimate users wishing to communicate securely. PKC security relies on exploiting the computational hardness of mathematical problems, such as discrete logarithm, and distributes the same session key to Alice and Bob. Symmetric encryption usually occurs in the upper layers, i.e., data link/MAC layer and above, allowing encryption of plaintext with the common session key shared between users using PKC.

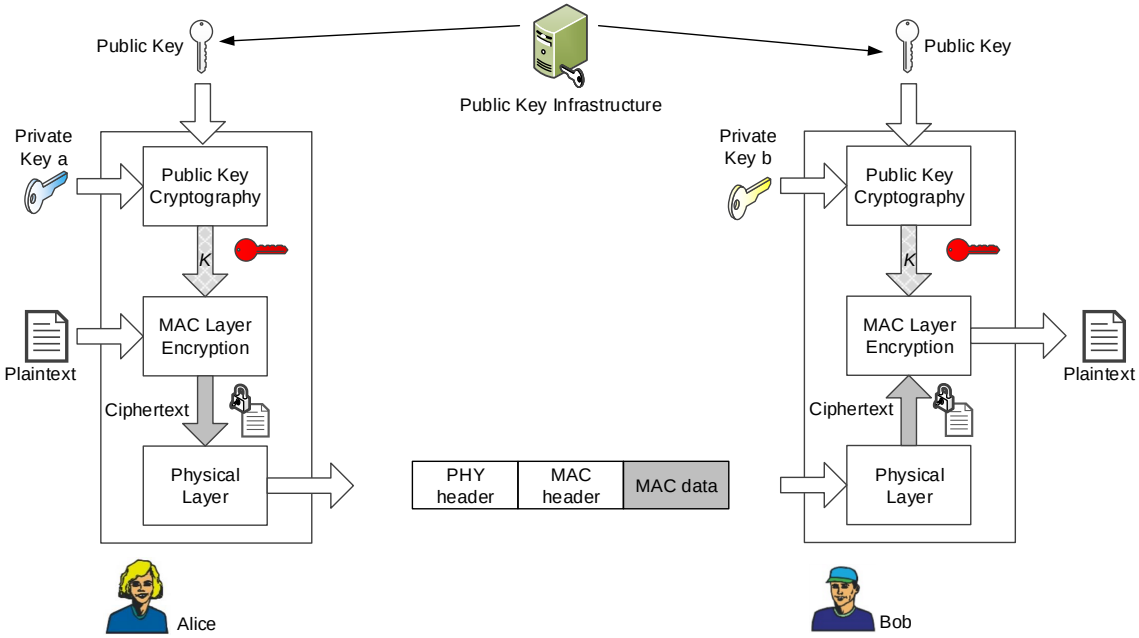

Figure 1. Classic cryptosystem with media access control (MAC) layer encryption as an example. The gray blocks represent the encrypted data.

Whilst classical cryptosystems have protected conventional wireless systems, there are challenges in applying these approaches in IoT. IoT devices range from well-resourced smartphones to low-cost, low energy and lightweight computing embedded devices. Many low-cost IoT devices cannot afford the additional silicon area, power consumption, and code space needed to perform the expensive mathematical calculations of cryptographic methodologies [17]. In addition, IoT applications may work in a device-to-device communication mode where there is no secured public key infrastructure (PKI) for the distribution of public keys. Finally, with the development of quantum computing, the concept of PKC will be fundamentally challenged [18].

Conventional upper layer-based cryptography also leaves the transmission vulnerable to many passive and active attacks. For example, the MAC header is sent in plaintext and attackers can perform traffic analysis by observing the MAC header. In addition, the physical packet header is also sent in plaintext and can reveal side-channel information (SCI) such as data rate, packet length, mapping

schemes, etc. [19]. Eavesdroppers can perform various attacks based on the observed SCI, such as analysis of users' activities and selective jamming.

Therefore, the design of a low-cost and robust cryptosystem for IoT is vital. While the main security streams have focused on the upper layers, the physical layer can also be leveraged to enhance security. In fact, reusing the physical layer features can decrease additional energy cost for security. As shown in Figure 2, security enhancement at the physical layer can be twofold. Firstly, information-theoretic security, also known as physical layer security (PLS), exploits the unpredictable features of wireless channels, such as fading; therefore, the system will not be compromised no matter how powerful the attackers are [20–23]. PLS transmission techniques achieve security through artificial noise [24], jamming [25], or beamforming [26], etc. However, many PLS transmission schemes are not practical yet because they require complex coding and/or the perfect/imperfect channel state information (CSI) of the receiver and/or eavesdroppers [13]. On the other hand, physical layer key generation, an active branch of PLS, is implementable because the legitimate users are able to agree on the same key from the noisy channel estimation [27], which can be used as an alternative to PKC in many circumstances. Secondly, moving the encryption to the physical layer can protect the entire physical layer packet and thus the wireless connection is secured from many passive and active attacks.

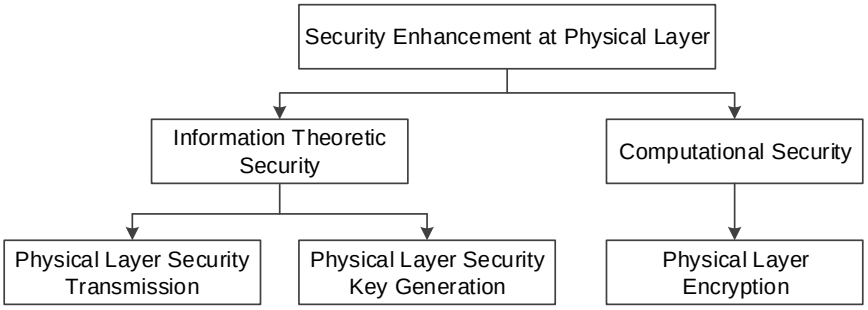

Figure 2. Taxonomy of security enhancement techniques at the physical layer.

Recently, a new hybrid approach considers how we can deploy cryptosystems directly into the physical layer and integrates information-theoretical security and computational security schemes, which are constructed by physical layer key generation and physical layer encryption (PLE), as shown in Figure 3. Alice and Bob carry out wireless transmission over the noisy channel using pilot signals. They are able to exploit common information of wireless channels and agree on the same cryptographic key through the key generation protocol that consists of channel probing, quantization, information reconciliation, and privacy amplification. The key is then fed to the PLE, which performs encryption operations at the modulation stages of the physical layer, and protects the IoT wireless transmission. Their integration offers a good example of how information-theoretic security schemes and computational security schemes can work together to protect IoT systems. Security countermeasures from the physical layer are lightweight and offer protection to the wireless transmission, and therefore are advantageous over conventional upper layer encryption-based security primitives.

There have been survey papers on the PLS transmission [28] and key generation [27,29] to protect IoT. However, PLS transmission is limited in practical implementation and a survey on integration of key generation and encryption has never been reported. This article aims to provide an overview on the recent progress of this promising hybrid physical layer cryptosystem, with a focus on the practical implementation and algorithm prototyping. The rest of this article is organized as follows. The wireless technologies used in IoT are introduced in Section 2. We then describe the physical layer key generation in Section 3 and PLE in Section 4. Finally, we propose some future research directions in Section 5 that make securing IoT from the physical layer more robust and pervasive. Section 6 concludes the article.

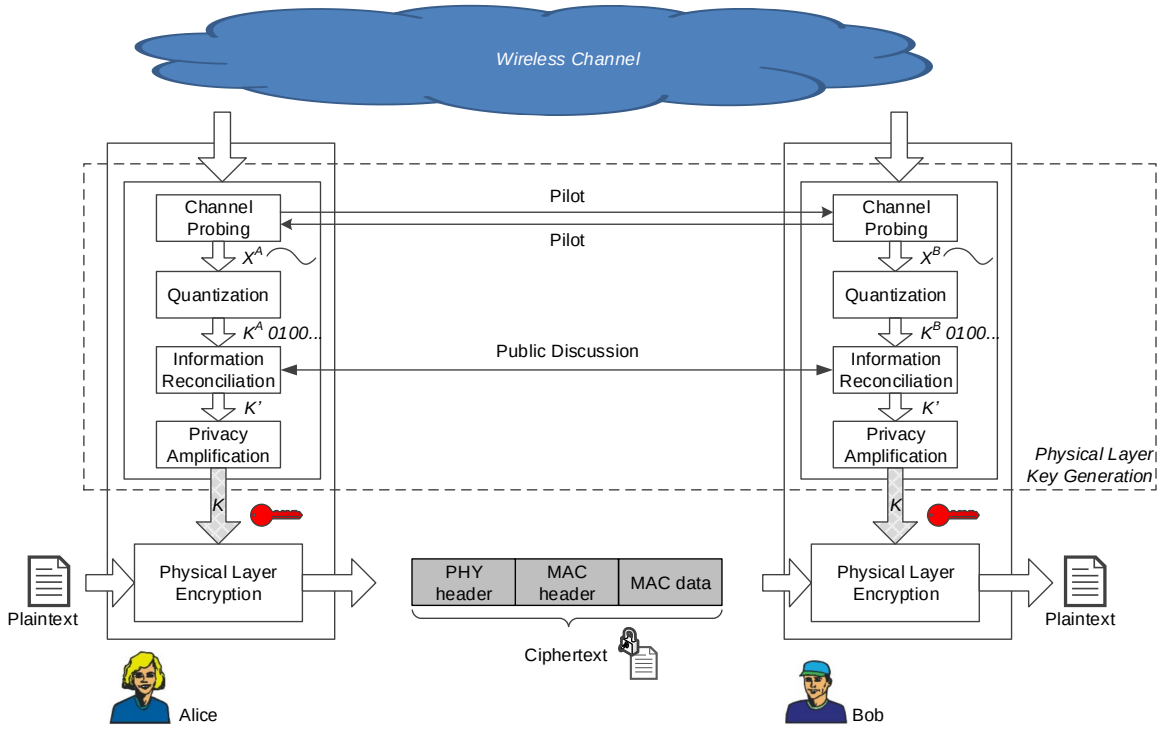

Figure 3. Key generation and physical layer encryption (PLE)-based cryptosystem. The gray blocks represent the encrypted data.

2. Wireless Technologies for IoT and Their Security Countermeasures

IoT aims to connect everything together and wireless communication is seen as the best option in order to avoid installation costs while enabling ubiquitous connection. IoT devices are normally tiny, embedded, and battery-powered, and thus communicate with each other through various low power wireless communication technologies. This section introduces several popular wireless technologies, including IEEE 802.15.4 (Zigbee), BLE, IEEE 802.11, and LoRaWAN.

IEEE 802.15.4 defines the physical and MAC layer protocols while Zigbee is based on IEEE 802.15.4 and includes high layer protocols. It runs at an unlicensed industrial, scientific and medical (ISM) 2.4 GHz frequency and uses direct sequence spread spectrum (DSSS) as the physical layer modulation. IEEE 802.15.4 is energy efficient and supports a data rate of up to 250 kbps, which is quite suitable for applications with limited data exchange requirements. It has been used extensively in wireless sensor networks (WSNs), especially in industrial applications.

BLE, also known as Bluetooth Smart, was standardized in 2010 as Bluetooth Core Specification Version 4.0. BLE runs at 2.4 GHz frequency and uses frequency hopping spread spectrum (FHSS) to combat frequency interference. It supports short range communications (50 to 100 m) and a data rate of 1 Mbps. In addition, BLE consumes extremely low energy and can run for months on standard coin-cell batteries. It is suited for IoT applications such as wearable devices and it is predicted by the Bluetooth special interest group that more than 90% smartphones will support BLE by 2018 [30].

IEEE 802.11 families are the most popular wireless local area network (WLAN) standards working at 2.4/5 GHz. They include IEEE 802.11a/b/g/n and are supported by almost all smartphones, laptops, tablets, etc. IEEE 802.11 can be used in smart home applications to provide large amounts of data transfer and as most houses are already covered by IEEE 802.11, installation costs can be avoided. Whilst legacy IEEE 802.11 standards may not be suitable for many lightweight IoT applications, IEEE 802.11ah was recently announced by the Wi-Fi alliance which has been developed explicitly for IoT. It works at sub 1 GHz bands and can cover large-range communications. In addition, 802.11ah adopts

narrower bandwidth and implements energy efficient protocols to extend the sensors' battery life. It is also optimized to support large groups of stations or sensors that cooperate to share the signals.

LoRaWAN is an emerging low power wide area network (WAN) technology with the first specification released in June, 2015 [31]. It also runs at sub 1 GHz and employs chirp spread spectrum. It supports long-range coverage (>15 km), millions of users, and low power consumption (up to ten years), and therefore is extremely suitable for low-cost IoT devices.

IEEE 802.15.4, Bluetooth, and IEEE 802.11 systems usually handle the security at the data link/MAC layer. For example, an AES block cipher is used to protect the link layer of IEEE 802.15.4 and Bluetooth systems. In IEEE 802.11 systems, an MAC layer encryption scheme named WPA has been designed and implemented using AES. LoRa implements the security countermeasures by encryption at network and application layers.

A summary and comparison of the wireless technologies for the IoT is given in Table 1.

Table 1. Wireless technologies for the Internet of Things (IoT).

Technique	Frequency	Range	Data Rate	Security Countermeasure	Applications
IEEE 802.15.4 (Zigbee)	2.4 GHz	10 to 100 m	250 kbps	AES in MAC layer	WSN, industrial, environment, and healthcare monitoring
BLE	2.4 GHz	50 to 150 m	1 Mbps	AES in link layer	Wearable devices, smartphones
IEEE 802.11 n/ac	2.4 or 5 GHz	50 m	> 100 Mbps	WPA in MAC layer (with AES implemented)	Smart home, entertainment
IEEE 802.11 ah	sub 1 GHz	1 km	150 kbps		Smart city, smart grid, smart home, healthcare,
LoRaWAN	sub 1 GHz	> 15 km	0.3 kbps to 50 kbps	Encryption at network and application layer	Machine-to-machine, smart city, and industrial applications

3. Physical Layer Key Generation

Key generation from the randomness of wireless channels has been receiving much research interest [27], as it is well suited for establishing cryptographic keys as an alternative to PKC in IoT applications [32]. As shown in Figure 3, firstly, key generation exploits unpredictable but characteristic features of the wireless channel, and is thus information-theoretically secure [33,34]. Secondly, it can be carried out between a pair of users with no aid from a third user, while a secured PKI is always required for PKC. Finally, key generation is lightweight and uses limited resources as all of the operations are not complicated and thus meets the low computation capacity of IoT devices. Zenger et al. implemented their key generation scheme in a 32-bit ARM Cortex M3 processor (EFM32GG-STK3700) and an 8-bit Intel MCS-51 and showed the resource and energy consumption to be very low [35]. The authors also implemented a lightweight PKC, elliptic curves Diffie–Hellman key generation (ECDH), as a comparison. As shown in Table 2, taking the implementation in a 32-bit ARM processor as an example, the ECDH requires 5.73 times more code, 128.26 times more cycles, and consumes 41.52 times more energy, than that of the key generation protocol, respectively. Therefore, key generation from wireless channels is extremely suitable for low-cost IoT devices.

Table 2. Resource and energy consumption comparison between key generation and elliptic curves Diffie–Hellman (ECDH).

Protocol	Platform	Architecture	Resources		Energy		
			Code Size (kb)	Cycles	Computation (mJ)	Communication (mJ)	Total (mJ)
Key generation	ARM Cortex-M3	32-bit	1.033	302,297	2.246	0.187	2.433
Key generation	Intel MCS-51	8-bit	1.137	1,345,205	5.206	0.187	5.393
ECDH	ARM Cortex-M3	32-bit	5.918	38,774,000	100.96	0.064	101.024
ECDH	Intel MCS-51	8-bit	8.749	1,734,400,000	528.45	0.064	528.514

Key generation works well in a dynamic wireless communication system, and is built on three principles.

- *Channel reciprocity* means the channel responses of the forward and backward links are the same, which is the basis for key generation. When two users measure the same channel parameters at the same frequency in a time-division duplex (TDD) mode, the measurements at Alice and Bob are impacted by the non-simultaneous sampling and noise. However, a high correlation between channel measurements of Alice and Bob can still be maintained and eligible for key generation in a slow fading channel, as demonstrated in many practical experiments [36–39].
- *Temporal variation* indicates that there is randomness residing in the dynamic channel, which ensures the extracted keys are random. A random key will make the cryptographic applications robust against attacks such as brute force. In the urban area, the interference may be chaotic, because of the densely deployed access points [40]. The interference will impact the channel measurements accuracy but will not affect randomness nature of the wireless link between users. In addition, the statistical features of the channel may be deterministic [41,42], but key generation is exploiting the instantaneous channel variation, which is random in nature.
- *Spatial decorrelation* implies that when located a half-wavelength away from the legitimate users, the eavesdropper experiences an uncorrelated channel compared to that between Alice or Bob, guaranteeing the security of the key generation. When the system works at 2.4 GHz, a half-wavelength is about 6 cm, which is quite short.

These principles have been theoretically modeled and analyzed in [43,44] and experimentally validated in [38,39].

3.1. Procedure

Key generation involves channel probing, quantization, information reconciliation, and privacy amplification, as shown in Figure 3. Without loss of generality, Alice is selected as the initiator of the key generation process.

In the channel probing step, the randomness residing in the temporal [36,37,43], frequency [43,45–47], and spatial [48–51] domains can be extracted by measuring the channel parameters such as the received signal strength (RSS) and CSI, etc. In particular, at time t_A, Alice sends a public pilot signal to Bob who will measure the channel parameter as X^B. Then, at time $t_B = t_A + \tau$, Bob also sends a public pilot signal to Alice who will measure the same channel parameter and store it as X^A. Alice and Bob will repeat the above channel sampling until they get enough measurements to generate a full set of keys. The key length is determined by the cryptographic applications. For example, the key length of AES can be 128-bit, 192-bit, or 256-bit. It is worth noting that in this step, users adopt a public pilot signal to measure the channel but do not try to exchange messages secretly. It is possible that some of the probe packets are not successful because of the poor channel condition, which results in a mismatch between the pairing of the measurements of Alice and Bob. This can be solved by exchanging and comparing the timestamps of the measurements, and keeping the records with the common timestamps. In TDD mode, the common timestamp does not necessarily indicate the timestamps with the exact same value, but their difference should be the sampling delay τ. For example, Alice will send her recorded timstamps to Bob, who will compare his timestamps and keep the common ones. Bob will then send his censored timestamps to Alice and she will also only keep the common ones, which will finally enable Alice and Bob to have the paired measurements. The exchange does not reveal any useful information to eavesdroppers.

In the second step, both Alice and Bob will convert the analog measurements into binary sequences using quantization schemes. Mean and standard deviation-based quantizer [36] (Algorithm 1) and cumulative distribution functions (CDF)-based quantizer [52] (Algorithm 2) are two popular quantizers. In Algorithm 1, μ_{X^u} is the mean value of X^u, σ_{X^u} is the standard deviation of X^u, α is used to adjust the threshold, and n is the number of the channel measurements. The design of the quantizer relies

on the selection of threshold and quantization level (QL). CDF-based quantization is able to obtain the same proportion of 0s and 1s as it can adaptively adjust the threshold, which is at the cost of increased complexity. The computational complexity of calculating the mean and variance is $\mathcal{O}(n)$. When calculating CDF, one key step is sorting the measurements, whose complexity is $\mathcal{O}(n\log(n))$, which requires more computation than the calculation of the mean and variance. A performance comparison of quantization schemes is reported in [53].

Algorithm 1 Mean and Standard Deviation-Based Quantization

INPUT: X^u % Channel measurement, RSS or CSI
OUTPUT: K^u % Key
$\eta_+^u = \mu_{X^u} + \alpha \times \sigma_{X^u}$ % η_+^u is the positive threshold.
$\eta_-^u = \mu_{X^u} - \alpha \times \sigma_{X^u}$ % η_-^u is the negative threshold.
for $i \leftarrow 1$ **to** n **do**
  if $X^u(i) > \eta_+^u$ **then**
    $K^u(i) = 1$
  else if $X^u(i) < \eta_-^u$ **then**
    $K^u(i) = 0$
  else
    $X^u(i)$ dropped
  end if
end for

Algorithm 2 CDF-Based Quantization

INPUT: X^u % Channel measurement, RSS or CSI
INPUT: QL % Quantization level
OUTPUT: K^u % Key
$F(x) = \Pr(X^u < x)$ % CDF calculation
$\eta_0^u = -\infty$ % Threshold
for $j \leftarrow 1$ **to** $2^{QL} - 1$ **do**
  $\eta_j^u = F^{-1}(\frac{j}{2^{QL}})$ % Threshold
end for
$\eta_{2^{QL}}^u = \infty$
Construct Gray code b_j and assign them to different intervals $[\eta_{j-1}^u, \eta_j^u]$
for $i \leftarrow 1$ **to** n **do**
  if $\eta_{j-1}^u \leq X^u(i) < \eta_j^u$ **then**
    $K^u(i, QL) = b_j$
  end if
end for

In practical measurements, due to the half-duplex nature of the most commercial hardware platforms and the independent hardware noise, channel measurements of Alice and Bob, i.e., X^A and X^B, will not be identical, thus resulting in a disagreement between K^A and K^B. In the information reconciliation stage, Alice and Bob will leverage the error correction code (ECC) to reach an agreement, which is achieved via public discussion by exchanging information such as the syndrome. Secure sketch [54] is a popular key reconciliation technique and is given as an example in Algorithm 3. A comprehensive survey on information reconciliation techniques can be found in [55]. Finally, privacy amplification is employed to eliminate the information revealed to eavesdroppers, which can be implemented using hash functions [27].

Algorithm 3 Secure Sketch

INPUT: K^A, K^B % Quantized keys of Alice and Bob
INPUT: C % ECC set shared by Alice and Bob
OUTPUT: K^A, $K^{B'}$ % Reconciled key
1: Alice randomly selects c from an ECC set C
2: Alice calculates $s = \text{XOR}(K^A, c)$
3: Alice transmits s to Bob through a public channel
4: Bob receives s
5: Bob calculates $c^B = \text{XOR}(K^B, s)$
6: Bob decodes c^B to get c
7: Bob calculates $K^{B'} = \text{XOR}(c, s) = K^A$ % Alice and Bob agree on the same key

3.2. Application

Due to its lightweight feature, this form of key generation has strong potential to provide the security for IoT. It has been applied in many wireless technologies, such as IEEE 802.11, IEEE 802.15.4, Bluetooth, etc., with many prototypes/implementations reported, see [27].

IEEE 802.11 is the most popular technique for the key generation implementation as the technique is widely adopted in our daily life. The work in [36] is one of the first and important papers that implemented key generation protocol. The authors generated keys from the peak of channel impulse response (CIR) using an 802.11 compatible field-programmable gate array (FPGA)-based platform, and also from RSS with a commercial Wi-Fi network interface card (NIC). However, the key generation rate is rather limited, i.e., about 1 bps, since the authors only extracted keys from the coarse-grained channel parameter. Orthogonal frequency-division multiplexing (OFDM) is employed by IEEE 802.11a/g/n/ah, which can provide fine-grained CSI in both time and frequency domain and significantly improve the key generation performance [43,45].

A key generation system using wearable devices with IEEE 802.15.4 is implemented in [56]. Channel measurements are carried out along with data transmission, in other words, no dedicated transmission is incurred for key generation. This avoids the additional energy burden required by key generation, which can significantly save power consumption as the radio transmission is always dominant [17]. In addition, a low-cost filter is employed to improve the signal cross-correlation, which helps the system reach an agreement as high as 99.8% [56]. Since there is not much data transmission required by wearable devices, the system takes about half an hour to generate 128-bit keys. The duration is acceptable as it still meets the requirement. For example, Wi-Fi recommends refreshing the session key every hour.

Key generation has also been applied in Bluetooth systems [57]. The authors implemented their system in two Google Nexus One smartphones and sampled RSS with experiments in indoor and outdoor environments. Random frequency hopping was employed to combat the interference from other wireless networks running at the ISM bands. It has also been demonstrated by experiments that Bluetooth-based key generation can be carried out using much lower transmit power (3 dBm) with a performance comparable to that of a Wi-Fi-based system, which is desirable for IoT devices.

4. Physical Layer Encryption

Modern communication systems employ a layered protocol stack to organize communication functions and most of the current security methodologies are applied at the MAC layer and above. The physical layer is the lowest layer of the protocol stack and was designed originally to modulate data for transmission but without any security considerations. This section introduces some recent ongoing encryption schemes implemented at the physical layer, which protects the entire physical layer packet. PLE schemes are lightweight as they do not introduce additional complexity, therefore are quite suitable for IoT applications.

4.1. Procedure

The data payload undergoes several physical layer modulation stages, such as channel coding, mapping, inverse fast Fourier transform (IFFT) operation (for OFDM systems), etc. PLE can be applied by encrypting the data flow in these physical layer modulation stages. Some PLE schemes applicable for OFDM systems are shown in Figure 4, including XOR encryption [58], phase encryption [58–60], and OFDM subcarriers encryption [61–67]. The user first generates the encryption information using the output of stream cipher or chaotic mapping. Based on the adopted encryption scheme, the encryption information is used to calculate phase rotation, dummy subcarrier locations, or subcarrier scrambling/interleaving permutation, etc., which is then used to protect the corresponding modulation stage. The detailed calculation step will be shown in Section 4.2. The seed for the stream cipher or the initial state of the chaotic map can be shared between legitimate users using the key generation discussed in the last section.

The entire packet is protected. The encryption of the physical layer payload, i.e., the MAC layer packet, will secure the MAC layer content, including the MAC header. In addition, the protection of the physical layer header can prevent eavesdroppers from carrying out functions of synchronization and channel estimation, significantly increasing the processing overheads for the eavesdropper [67].

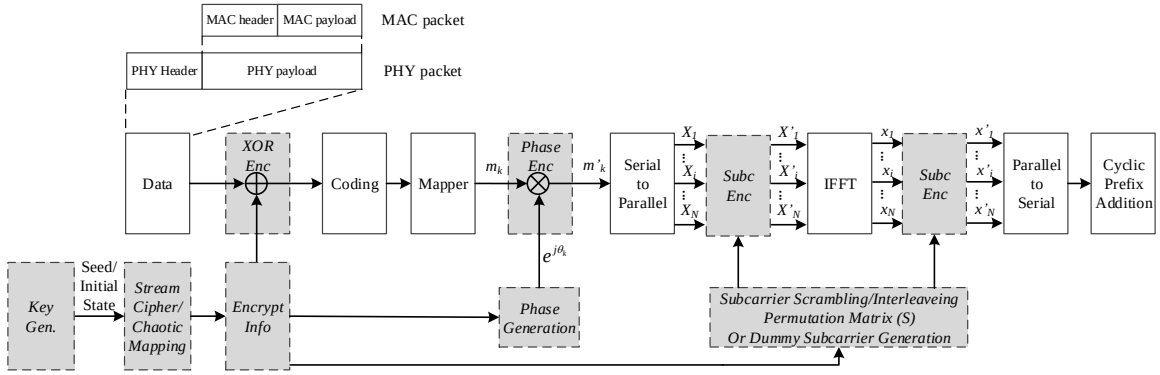

Figure 4. Physical layer encryption schemes in orthogonal frequency-division multiplexing (OFDM). Gray modules are added for encryption.

4.2. Algorithm Prototype

The PLE design is determined by the wireless technologies which employ different physical layer modulations. In this section, we introduce several PLE prototypes based on the modulation stage that they have encrypted.

XOR encryption is the most straightforward and lightweight scheme and can be implemented in hardware in a very efficient manner. As XOR is a bitwise operation, it usually happens before coding, as shown in Figure 4. This scheme is applicable to all the wireless technologies as the data passed from the MAC layer is always in binary form. However, it is implemented at the beginning of modulation stages and does not randomize the physical layer waveform, which results in a weaker protection [67].

Phase encryption can also be applied as long as phase-shift keying or quadrature amplitude modulation is used [58–60]. As shown in Figure 4, phase encryption occurs after symbol mapping and the constellation symbols are not in binary values any more. The encrypted constellation symbols m'_k can be denoted as

$$m'_k = m_k e^{j\theta_k} + n_k, \tag{1}$$

where m_k is the constellation symbols, θ_k is the rotation angle, and n_k is the random noise. θ_k is generated according to the key sequence and then used to rotate the constellation symbols. In order to create a denser encrypted constellation, more key bits are required to generate rotation angles, which

increases the key-to-data ratio, defined as the number of key bits needed to encrypt one bit plaintext. Random noise, n_k, can be deliberately added to the rotated symbols to make it even more difficult for the eavesdroppers to demodulate the ciphertext [59,60]. The implementation of this technique is also efficient because the main resource is a multiplier and related control circuits. The OFDM technique modulates data onto multiple orthogonal subcarriers/frequencies and can significantly increase the data rate, providing an additional domain to protect the data. The parallel input data X can be scrambled in the frequency domain before IFFT operation [61–63], which can be given as

$$X' = XS_f, \tag{2}$$

where S_f is the frequency scrambling matrix, or the IFFT output data can be scrambled in the time domain [64] and written as

$$x' = xS_t, \tag{3}$$

where S_t is the time scrambling matrix. Scramble-based schemes can bring a large search space. However, it may result in a high computational complexity as matrix operations are required, which may not be suitable for low-cost devices [67].

Different from above OFDM schemes that scramble all the data subcarriers, the work in [65,66] interleaves only part of the subcarriers. In particular, the scheme in [65] selects a subset of the subcarriers whose phase is larger than the threshold, and then interleaves their real and imaginary components of the symbols. The method in [66] selects a subcarrier subset based on the CSI, and then interleaves these subcarriers according to the descending order of their channel amplitudes. Encryption usually involves mathematical operations, e.g., XOR operation, between the plaintext and key sequence, but here the concept applies more generally to the data manipulation according to the common secret information. In addition, the authors use channel information as encryption information directly without resorting to stream ciphers, which requires a careful design of the interleaving pattern because of the channel estimation errors at transmitters and receivers.

While the standard OFDM systems use all the data subcarriers for data transmission, some subcarriers can also be reserved to transmit dummy data, i.e., rubbish information, for obfuscation [67]. Due to the introduction of dummy subcarriers, there is a trade-off between the security and data rate, but it has been demonstrated in [67] that it is worthwhile as there are many subcarriers and the data rate is usually only slightly reduced. In addition, the preambles are encrypted in [67] so the entire packet is protected.

The above schemes protect different physical layer modulation stages, which lead to distinctions on the security level, complexity, etc. For example, XOR and phase encryption are easier to implement but provide less strong protection. On the other hand, scrambling-based schemes may require matrix operations, including matrix multiplication and inversion, which result in a higher computation complexity. A detailed comparison in terms of search space to the brute force attack, key rate, and complexity of the above schemes can be found in [67].

4.3. Practical Implementation

To the best of the authors' knowledge, there has been only one paper which has implemented a physical layer phase encryption IEEE 802.15.4 transceiver and RC4 to generate the key sequence [68]. The work in [68] first validated the design using FPGA technology and then implemented the system in an application-specific integrated circuit (ASIC) using UMC 0.18 µm complementary metal-oxide-semiconductor (CMOS) technology. The security enhancement, including the RC4 and phase encryption/decryption, results in a 26% increase on the gate counts compared to a standard 802.15.4 transceiver, which is a reasonable overheard for security.

5. Future Work Suggestions

Although there have been prototypes/demonstrations of the above physical layer-based security countermeasures, research is still needed to make these schemes more robust and pervasive. In this section, we suggest some future research directions in securing the IoT from the physical layer.

5.1. Physical Layer Key Generation

Most current commercial platforms work in half-duplex mode, and the keying nodes have to measure the channel alternately in different time instances. Key generation in this setting is only applicable to slow fading channels in order to get highly correlated measurements between users. Therefore, key generation in fast fading channels is very challenging, which limits its application, e.g., in vehicular communications. Work in [69] and [70] designed key generation systems with the maximum vehicle speed tested as 20 mph and 50 mph, respectively, but their key generation rates are limited, e.g., 5 bit/s in [70]. In addition, work in [71] tested their algorithms in an indoor environment only. There is also some simulation work, e.g., [72,73]. Their performance in the practical fast fading channels remains unknown. This topic thus still requires more efforts, e.g., by using full-duplex hardware [74].

Efficient group and pairwise key generation are essential to assist secure broadcast and unicast transmission in a large-scale IoT network. A fusion center broadcasts signals to the network users, which requires a pre-establishment of a common session key. The devices may also exchange unicast packets between each other, and private keys between pairs of users are required. In ad hoc IoT, many users may join and leave the network frequently, therefore robust and efficient schemes to update the session key and private keys are required. There have been several group key generation protocols reported, e.g., a time-slotted round-trip phase-based scheme [75], RSS-based protocols for star and chain topologies [76], and group key generation for mesh topology [77]. However, the scalability (with the size of the group) and efficiency of the above protocols are limited and more research effort is required.

Although key generation is able to achieve information-theoretic security, in practice the security performance requires special attention. For example, when there is a strong line-of-sight, the spatial decorrelation may not hold any more, which makes the system vulnerable to passive eavesdropping [39,78]. Key generation is also subject to active attacks [79,80], which will result in less efficient or even unsuccessful key generation. It is thereof very important to design key generation techniques secure from passive eavesdropping and robust to active jamming. In addition, the majority of the research focuses on the indoor and/or mobile channels, while in an outdoor or static environment, the channel randomness is rather limited. A less random key will expose the cryptographic systems to brute force attack and should always be avoided.

5.2. Physical Layer Encryption

PLE applies encryption at the physical layer, and entails additional operations and hardware resources. No hardware implementation for PLE schemes has been reported except for those in [68]. The additional operations will introduce latency in the critical path and may not meet the timing requirements of the current MAC protocol. Therefore, a cross-layer design between the physical and MAC layer is necessary.

The keys generated are usually fed to a stream cipher to produce pseudo random numbers to encrypt plaintext. In scenarios where keys can be generated fast or only very small amount of data exchange is required, the keys generated can be used to encrypt the data directly, rather than be used as the seed for stream cipher. Key generation and PLE is then integrated as a one-time pad scheme to offer perfect Shannon secrecy, which can provide the strongest protection ever. However, the practical security performance and implementation require further investigation.

6. Conclusions

This article has provided an overview of securing wireless communications of IoT applications from the physical layer. We have introduced two security techniques, namely, physical layer key generation and physical layer encryption. For each, we have discussed their features and applications by a special consideration of IoT devices' low power and low-cost features. The remaining challenges of how to make these schemes more robust and pervasive have also been proposed. Unlike previous work, this article has focused on practical prototypes/implementations, thus offering insights into their applications in the IoT to enhance wireless security.

Acknowledgments: This work was supported by the Royal Society Research Grant under Grant ID RG160302.

Author Contributions: All the authors contributed equally to the paper writing, revision, correction and proof reading.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ASIC	Application-specific integrated circuit
BLE	Bluetooth low power
CDF	Cumulative distribution functions
CIR	Channel impulse response
CMOS	Complementary metal-oxide-semiconductor
CSI	Channel state information
DSSS	Direct sequence spread spectrum
ECC	Error correction code
FPGA	Field-programmable gate array
IEEE	The Institute of Electrical and Electronics Engineers
IFFT	Inverse fast Fourier transform
IoT	Internet of Things
ISM	Industrial, scientific and medical
FHSS	Frequency hopping spread spectrum
MAC	Media access control
NFC	Near field communication
NIC	Network interface card
OFDM	Orthogonal frequency-division multiplexing
PKC	Public key cryptography
PKI	Public key infrastructure
PLE	Physical layer encryption
PLS	Physical layer security
RFID	Radio-frequency identification
RSS	Received signal strength
SCI	Side-channel information
TDD	Time-division duplex
TLS	Transport layer security
Wi-Fi	Wireless fidelity
WLAN	Wireless local area network
WPA	Wi-Fi protected access
WSN	Wireless sensor network

References

1. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805.
2. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surveys Tuts.* **2015**, *17*, 2347–2376.

3. Stankovic, J.A. Research directions for the internet of things. *IEEE Internet Things J.* **2014**, *1*, 3–9.
4. Walport, M. The Internet of Things: Making the most of the Second Digital Revolution, A report by the UK Government Chief Scientific Adviser. Technical Report, 2014. Available online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf (accessed on 22 June 2017).
5. The Internet of Things: Five critical questions, 2015. Available online: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-five-critical-questions (accessed on 22 June 2017).
6. A Partnership to Secure and Protect the Emerging Internet of Things, 2015. Available online: http://nsf.gov/news/news_summ.jsp?cntn_id=136104&org=NSF (accessed on 22 June 2017).
7. IERC—European Research Cluster on the Internet of Things. Available online: http://www.internet-of-things-research.eu/ (accessed on 22 June 2017).
8. New Internet of Things Research Hub Announced, 2016. Available online: https://www.epsrc.ac.uk/newsevents/news/iotresearchhub/ (accessed on 22 June 2017).
9. Nordrum, A. The Internet of Fewer Things, 2016. Available online: http://spectrum.ieee.org/telecom/internet/the-internet-of-fewer-things (accessed on 22 June 2017).
10. Evans, D. Internet Of Things Research Study. Technical Report, Cisco, 2011. Available online: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 22 June 2017).
11. Grau, A. How to Build a Safer Internet of Things, 2015. Available online: http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things (accessed on 22 June 2017).
12. Internet of things research study. Technical report, HP, 2015. Available online: https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA5-4759ENN.pdf (accessed on 22 June 2017).
13. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765.
14. Granjal, J.; Monteiro, E.; Sa Silva, J. Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Commun. Surveys Tuts.* **2015**, *17*, 1294–1312.
15. Dieks, T.; Rescorla, E. The Transport Layer Security (TLS) Protocol. Available online: https://tools.ietf.org/html/rfc5246 (accessed on 17 August 2017).
16. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*; Technical Report 802.11i; IEEE: Piscataway, NJ, USA, 2004.
17. Trappe, W.; Howard, R.; Moore, R.S. Low-Energy Security: Limits and Opportunities in the Internet of Things. *IEEE Secur. Priv.* **2015**, *13*, 14–21.
18. Cheng, C.; Lu, R.; Petzoldt, A.; Takagi, T. Securing the Internet of Things in a Quantum World. *IEEE Commun. Mag.* **2017**, *55*, 116–120.
19. Rahbari, H.; Krunz, M. Secrecy beyond encryption: Obfuscating transmission signatures in wireless communications. *IEEE Commun. Mag.* **2015**, *53*, 54–60.
20. Zhou, X.; Song, L.; Zhang, Y. *Physical Layer Security in Wireless Communications*; CRC Press: Boca Raton, FL, USA, 2013.
21. He, B.; Zhou, X.; Abhayapala, T.D. Wireless physical layer security with imperfect channel state information: A survey. *ZTE Commun.* **2013**, *11*, 11–19.
22. Mukherjee, A.; Fakoorian, S.; Huang, J.; Swindlehurst, A. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surveys Tuts.* **2014**, *16*, 1550–1573.
23. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, Technologies, and Challenges. *IEEE Commun. Surveys Tuts.* **2017**, *19*, 347–376.
24. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.* **2008**, *7*, 2180–2189.
25. Ma, S.; Hempel, M.; Yang, Y.L.; Sharif, H. An approach to secure wireless communications using randomized eigenvector-based jamming signals. In Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, Caen, France, 28 June–2 July 2010; pp. 1172–1176.
26. Mukherjee, A.; Swindlehurst, A.L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans. Signal Process.* **2011**, *59*, 351–361.

27. Zhang, J.; Duong, T.Q.; Marshall, A.; Woods, R. Key Generation from Wireless Channels: A Review. *IEEE Access* **2016**, *4*, 614–626.
28. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761.
29. Zeng, K. Physical layer key generation in wireless networks: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 33–39.
30. Janiak, S. Three Ways Bluetooth® Smart Technology Enables Innovation for the Internet of Things, 2015. Available online: http://blog.bluetooth.com/three-ways-bluetooth-smart-technology-enables-innovation-for-the-internet-of-things/ (accessed on 22 June 2017).
31. LoRa Alliance. Available online: https://www.lora-alliance.org/ (accessed on 22 June 2017).
32. Zenger, C.T.; Chur, M.J.; Posielek, J.F.; Paar, C.; Wunder, G. A Novel Key Generating Architecture for Wireless Low-Resource Devices. In Proceedings of the 2014 International Workshop on Secure Internet of Things (SIoT), Wroclaw, Poland, 10 September 2014; pp. 26–34.
33. Ahlswede, R.; Csiszar, I. Common randomness in information theory and cryptography—Part I: Secret sharing. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132.
34. Maurer, U.M. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742.
35. Zenger, C.T.; Pietersz, M.; Zimmer, J.; Posielek, J.F.; Lenze, T.; Paar, C. Authenticated key establishment for low-resource devices exploiting correlated random channels. *Comput. Netw.* **2016**, *109*, 105–123.
36. Mathur, S.; Trappe, W.; Mandayam, N.; Ye, C.; Reznik, A. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom), San Francisco, CA, USA, 14–19 September 2008; pp. 128–139.
37. Jana, S.; Premnath, S.N.; Clark, M.; Kasera, S.K.; Patwari, N.; Krishnamurthy, S.V. On the effectiveness of secret key extraction from wireless signal strength in real environments. In Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom), Beijing, China, 20–25 September 2009; pp. 321–332.
38. Zhang, J.; Woods, R.; Duong, T.Q.; Marshall, A.; Ding, Y. Experimental Study on Channel Reciprocity in Wireless Key Generation. In Proceedings of the 17th IEEE International Workshop Signal Processing Advances in Wireless Communications (SPAWC), Edinburgh, UK, 3–6 July 2016; pp. 1–5.
39. Zhang, J.; Woods, R.; Duong, T.Q.; Marshall, A.; Ding, Y.; Huang, Y.; Xu, Q. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access* **2016**, *4*, 4464–4477.
40. Kajita, S.; Amano, T.; Yamaguchi, H.; Higashino, T.; Takai, M. Wi-Fi Channel Selection Based on Urban Interference Measurement. In Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Hiroshima, Japan, 28 November–1 December 2016; pp. 143–150.
41. Chin, E.; Chieng, D.; Teh, V.; Natkaniec, M.; Loziak, K.; Gozdecki, J. Wireless link prediction and triggering using modified Ornstein–Uhlenbeck jump diffusion process. *Wirel. Netw.* **2014**, *20*, 379–396.
42. Santana, J.A.; Macías, E.; Suárez, Á.; Marrero, D.; Mena, V. Adaptive estimation of WiFi RSSI and its impact over advanced wireless services. In *Mobile Networks and Applications*; Springer Science+Business Media: New York, NY, USA, 2016; pp. 1–13.
43. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Efficient Key Generation by Exploiting Randomness from Channel Responses of Individual OFDM Subcarriers. *IEEE Trans. Commun.* **2016**, *64*, 2578–2588.
44. Zhang, J.; He, B.; Duong, T.Q.; Woods, R. On the Key Generation from Correlated Wireless Channels. *IEEE Commun. Lett.* **2017**, *21*, 961–964.
45. Liu, H.; Wang, Y.; Yang, J.; Chen, Y. Fast and practical secret key extraction by exploiting channel response. In Proceedings of the 32nd IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 3048–3056.
46. Xi, W.; Li, X.; Qian, C.; Han, J.; Tang, S.; Zhao, J.; Zhao, K. KEEP: Fast secret key extraction protocol for D2D communication. In Proceedings of the 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), Hong Kong, China, 26–27 May 2014; pp. 350–359.
47. Peng, Y.; Wang, P.; Xiang, W.; Li, Y. Secret Key Generation Based On Estimated Channel State Information for TDD-OFDM Systems Over Fading Channels. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5176–5186.

48. Zeng, K.; Wu, D.; Chan, A.; Mohapatra, P. Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In Proceedings of the 29th IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
49. Wallace, J.W.; Sharma, R.K. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 381–392.
50. Chen, C.; Jensen, M.A. Secret key establishment using temporally and spatially correlated wireless channel coefficients. *IEEE Trans. Mobile Comput.* **2011**, *10*, 205–215.
51. Jorswieck, E.A.; Wolf, A.; Engelmann, S. Secret key generation from reciprocal spatially correlated MIMO channels. In Proceedings of the IEEE GLOBECOM Workshop Trusted Communications with Physical Layer Security (TCPLS), Atlanta, GA, USA, 9–13 December 2013; pp. 1245–1250.
52. Patwari, N.; Croft, J.; Jana, S.; Kasera, S.K. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. *IEEE Trans. Mobile Comput.* **2010**, *9*, 17–30.
53. Zenger, C.T.; Zimmer, J.; Paar, C. Security Analysis of Quantization Schemes for Channel-based Key Extraction. In Proceedings of the 12th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Coimbra, Portugal, 22–24 July 2015; pp. 267–272.
54. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM J. Comput.* **2008**, *38*, 97–139.
55. Huth, C.; Guillaume, R.; Strohm, T.; Duplys, P.; Samuel, I.A.; Güneysu, T. Information reconciliation schemes in physical-layer security: A survey. *Comput. Netw.* **2016**, *109*, 84–104.
56. Ali, S.; Sivaraman, V.; Ostry, D. Eliminating Reconciliation Cost in Secret Key Generation for Body-Worn Health Monitoring Devices. *IEEE Trans. Mobile Comput.* **2014**, *13*, 2763–2776.
57. Premnath, S.N.; Gowda, P.L.; Kasera, S.K.; Patwari, N.; Ricci, R. Secret key extraction using Bluetooth wireless signal strength measurements. In Proceedings of the 11th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Singapore, 30 June–3 July 2014; pp. 293–301.
58. Huo, F.; Gong, G. XOR encryption versus phase encryption, An in-depth analysis. *IEEE Trans. Electromagn. Compat.* **2015**, *57*, 903–911.
59. Reilly, D.; Kanter, G. Noise-enhanced encryption for physical layer security in an OFDM radio. In Proceedings of the IEEE Radio and Wireless Symposium (RWS), San Diego, CA, USA, 18–22 January 2009; pp. 344–347.
60. Ma, R.; Dai, L.; Wang, Z.; Wang, J. Secure communication in TDS-OFDM system using constellation rotation and noise insertion. *IEEE Trans. Consum. Electron.* **2010**, *56*, 1328–1332.
61. Khan, M.A.; Asim, M.; Jeoti, V.; Manzoor, R.S. On secure OFDM system: Chaos based constellation scrambling. In Proceedings of the International Conference on Intelligent and Advanced Systems (ICIAS), Kuala Lumpur, Malaysia, 25–28 November 2007; pp. 484–488.
62. Tseng, D.; Chiu, J. An OFDM speech scrambler without residual intelligibility. In Proceedings of the IEEE Region 10 Conference (TENCON), Taipei, Taiwan, 30 October–2 November 2007; pp. 1–4.
63. Zhang, L.; Xin, X.; Liu, B.; Wang, Y. Secure OFDM-PON based on chaos scrambling. *IEEE Photon. Technol. Lett.* **2011**, *23*, 998–1000.
64. Li, H.; Wang, X.; Hou, W. Secure transmission in OFDM systems by using time domain scrambling. In Proceedings of the 77th IEEE Vehicular Technology Conference (VTC Spring), Dresden, Germany, 2–5 June 2013; pp. 1–5.
65. Li, H.; Wang, X.; Zou, Y. Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems. *IEEE Commun. Lett.* **2014**, *18*, 1059–1062.
66. Li, H.; Wang, X.; Chouinard, J.Y. Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 1155–1165.
67. Zhang, J.; Marshall, A.; Woods, R.; Duong, T.Q. Design of an OFDM Physical Layer Encryption Scheme. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2114–2127.
68. Nain, A.K.; Bandaru, J.; Zubair, M.A.; Pachamuthu, R. A Secure Phase-Encrypted IEEE 802.15.4 Transceiver Design. *IEEE Trans. Comput.* **2017**, *66*, 1421–1427.
69. Wan, J.; Lopez, A.B.; Al Faruque, M.A. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. In Proceedings of the 7th International Conference on Cyber-Physical Systems, Vienna, Austria, 11–14 April 2016; p. 13.

70. Zhu, X.; Xu, F.; Novak, E.; Tan, C.C.; Li, Q.; Chen, G. Using Wireless Link Dynamics to Extract a Secret Key in Vehicular Scenarios. *IEEE Trans. Mobile Comput.* **2017**, *16*, 2065–2078.
71. Li, X.; Liu, J.; Yao, Q.; Ma, J. Efficient and Consistent Key Extraction Based on Received Signal Strength for Vehicular Ad Hoc Networks. *IEEE Access* **2017**, *5*, 5281–5291.
72. Abdelgader, A.M.; Wu, L. A secret key extraction technique applied in vehicular networks. In Proceedings of the IEEE International Conference on Computational Science and Engineering, Chengdu, China, 19–21 December 2014; pp. 1396–1403.
73. Abdelgader, A.M.S.; Feng, S.; Wu, L. Exploiting the Randomness Inherent of the Channel for Secret Key Sharing in Vehicular Communications. *Int. J. Intell. Transp. Syst. Res.* **2017**, doi:10.1007/s13177-017-0136-4.
74. Vogt, H.; Ramm, K.; Sezgin, A. Practical Secret-Key Generation by Full-Duplex Nodes with Residual Self-Interference. In Proceedings of the 20th International ITG Workshop on Smart Antennas (WSA 2016), Munich, Germany, 9–11 March 2016; pp. 344–347.
75. Wang, Q.; Su, H.; Ren, K.; Kim, K. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In Proceedings of the 30th IEEE (INFOCOM), Shanghai, China, 10–15 April 2011; pp. 1422–1430.
76. Liu, H.; Yang, J.; Wang, Y.; Chen, Y.J.; Koksal, C.E. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation. *IEEE Trans. Mobile Comput.* **2014**, *13*, 2820–2835.
77. Thai, C.D.T.; Lee, J.; Quek, T.Q. Secret group key generation in physical layer for mesh topology. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; pp. 1–6.
78. Zenger, C.; Vogt, H.; Zimmer, J.; Sezgin, A.; Paar, C. The Passive Eavesdropper Affects My Channel: Secret-Key Rates under Real-World Conditions. In Proceedings of the IEEE GLOBECOM Workshop Trusted Communications with Physical Layer Security (TCPLS), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
79. Zafer, M.; Agrawal, D.; Srivatsa, M. Limitations of generating a secret key using wireless fading under active adversary. *IEEE/ACM Trans. Netw.* **2012**, *20*, 1440–1451.
80. Jin, R.; Zeng, K. Physical layer key agreement under signal injection attacks. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Florence, Italy, 28–30 September 2015; pp. 254–262.